



# SAFEGUARD

A quarterly newsletter published by the Office of the Information and Privacy  
Commissioner

Volume 8, Issue 1

February 2024

## Contact Information

Office of the Information  
and Privacy Commissioner

3<sup>rd</sup> Floor, 2 Canada Drive  
Sir Brian Dunfield Building  
P.O. Box 13004, Station A  
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland  
and Labrador:

1-877-729-6309

Email:

[commissioner@oipc.nl.ca](mailto:commissioner@oipc.nl.ca)

Website:

[www.oipc.nl.ca](http://www.oipc.nl.ca)

## Follow us on social media!

Twitter:

[@oipcnl](https://twitter.com/@oipcnl)

LinkedIn:

[https://LinkedIn.com/  
pany/oipc-nl](https://LinkedIn.com/company/oipc-nl)

## This Issue:

- Personal Health Record
- Small Custodians and the Use of Artificial Intelligence
- Protecting Personal Health Information Off-Site or On the Road
- *PHIA* Privacy Breach Statistics November 1, 2023 – January 31, 2024

## Personal Health Record

The Provincial Government and Newfoundland and Labrador Health Services (NL Health Services) announced at the end of January that they are introducing a new online service to improve access to the health care system.

The personal health record is an online service that will allow residents to access their health information. It will be available through [MyGovNL](#) and it will give residents access to:

- laboratory results;
- dispensed medications;
- radiology reports; and
- allergies.

This online service will initially be available starting on February 1, 2024 to a small group, up to 5,000 people who are 16 years of age and older. However, in the following months, the service will be increased to groups of 50,000 residents.

It was also announced that an app is being developed for release this coming spring that will incorporate the personal health record and will allow residents to check on information related to prescribed medication, refills of medication and have more informed discussions with their health care providers. In future, updates to the app will provide additional services such as the ability to schedule medical appointments with NL Health Services, including with family care teams and participating physicians.

For more information on the Provincial Government's recent health care actions, please visit [healthcareaction.ca](http://healthcareaction.ca).

## Small Custodians and the Use of Artificial Intelligence

The Office of the Information and Privacy Commissioner for Alberta produced a guidance piece on artificial intelligence (AI) and small custodians - [AI: Guidance for Small Custodians on the use of Artificial Intelligence](#).

We will touch on parts of this guidance below to help small custodians consider the risks if they use AI systems in their practices. Similar to Alberta, Newfoundland and Labrador has no specific laws regulating the use of AI. While Newfoundland and Labrador's legislation governing personal health information is different from Alberta's legislation, aspects of this guidance are still relevant for custodians in this province.

### What is AI and what are AI systems?

AI is an advanced form of information processing for the purpose of automating and/or enhancing the performance of human tasks. AI is a catch-all for various kinds of techniques to process information in a way that resembles human intelligence. AI always requires three ingredients, which are:

- hardware, to provide the infrastructure, storage and processing power;
- software, computer code to resemble intelligent interaction with whatever inputs are provided; and
- data, as an input to generate a useful output and to train the software in the first place.

An AI system is a product or service used by an entity, which utilizes a form of AI to automate, enhance or otherwise improve or facilitate service delivery.

### How is AI used in Healthcare?

AI is being used in health care to assist in various areas, including drug discovery and development, enhancing medical devices, diagnosing patients, scheduling patients, transcribing medical documents and helping improve physician-patient communication. A majority of AI applications in health care involve the processing of personal health information and sometimes personal information (e.g. employee information).

### The Personal Health Information Act and Legal Authority

Newfoundland and Labrador's *Personal Health Information Act (PHIA)* governs the collection, use, and disclosure of personal health information. A custodian in Newfoundland and Labrador is required to comply with *PHIA* regardless of whether they use AI systems.

It is important to familiarize yourself with how the AI technology works. Is the personal health information being processed solely to provide care, or are there secondary purposes such as reinforcing the learning of the AI system, system technical diagnostics and performance of the AI, identifying sales or marketing opportunities, etc.?

When AI systems interact with personal health information, there are requirements for using these systems. You may not have legal authority for some of the purposes proposed by the system's service provider. Once the information about purposes is known, you must ensure that you have the authority to collect, use and disclose personal health information for each of the identified

purposes. If you do not have authority for a purpose, you need to work with the technology provider to customize the service delivered or limit the use or disclosure of information for secondary purposes, to ensure you meet your obligations under *PHIA*.

### Compliance Risk

AI systems carry compliance risks, which are inherent to all information and communication technology (ICT) systems. You need to ensure you meet your security obligations under *PHIA* by having reasonable physical, administrative, and technical controls in place on the use of all your ICT systems. You also need to consider how you will comply with requirements for providing access to information and for responding to an individual who requests correction of their information.

If a custodian is planning to use an AI system to process personal health information, they must assess their duties under *PHIA* to collect, use, and disclose personal health information in accordance with the law. They must also ensure their practices are in compliance with requirements regarding security of, access to, and retention of personal health information.

A privacy impact assessment (PIA) is useful to help identify privacy and security risks and ensure they are addressed prior to the implementation of AI systems that process personal health information.

### Questions to Consider Before Acquiring AI Services

There are benefits that can result from the use of AI, including improved productivity, enhanced delivery of traditional health care, and optimization of the clinical services being provided. Custodians can do their part to prevent adverse effects by asking questions and gathering the right information before implementing an AI system.

- What is the purpose of the AI system I want to obtain?
  - Is this process better done by AI, by a human or by a combination of both?
  - What is the balance of costs, risks and benefits?
  - What is the impact of using AI for this process for me, my staff and my patients?
- What data will be used by the AI system? Will this data include personal health information?
- Do I have authority under *PHIA* to process personal health information with this AI system?
- What are the guarantees, certifications, policies and contractual obligations of the service provider that offers the AI system?
  - Are adequate physical, administrative and technical safeguards in place?
  - Do the certifications, policies, and contractual obligations meet or exceed the compliance requirements?
  - Do I have a clear idea of the risks of the product or service, and are there contingency plans in place for any risks?
  - If the service provider of the AI system claims that only anonymized or non-identifying personal health information is used for secondary purposes, what standard for anonymization or de-identification is being used and do the service provider's practices guarantee that there is no risk of re-identification?
  - Has the service provider assessed and taken proper steps to assure the accuracy and fairness of the product or service (e.g. bias of training data and bias of outcomes).

- Is the personal health information processed outside of Newfoundland and Labrador or Canada?
- How is the personal health information secured when used by the AI system?
  - Where is the personal health information stored? Is it stored in a cloud-based service?
  - Is the personal health information encrypted in transit and in storage using industry standard algorithms? Are the encryption keys securely managed and by whom?
  - Was the AI system reasonably tested prior to and after your implementation? Are both the AI software and the infrastructure it runs on continuously monitored for security issues?
- Will personal health information be used to train the AI system I use?
- How do I prepare for the use of an AI system in my practice?
  - What additional AI-specific training, policies, and procedures do I need to implement?
  - Is it transparent to patients that AI is or will be used, and how it is used?
  - Can patients opt out of having their information processed by AI and can they request a second opinion, if they disagree with results?

Our Office publishes guidance to help custodians comply with *PHIA*. All resources can be found on our website at [www.oipc.ni.ca](http://www.oipc.ni.ca) and specifically the [PHIA Toolkit for Small Custodians](#) and the [PHIA Compliance Checklist for Custodians](#) are great resources.

## Protecting Personal Health Information Off-Site or On the Road

There are times when a custodian will have personal health information with them, if they are working outside their office or possibly commuting between locations. Here are some tips and considerations to help keep personal health information secure while a custodian is off-site or on the road.

### What is the Custodian's Responsibility?

Under *PHIA*, custodians are required to keep personal health information secure. Custodians must ensure they are adequately protecting an individual's personal health information at all times.

A custodian must take reasonable steps to ensure that:

- personal health information in its custody or control is protected against theft, loss, and unauthorized access, use or disclosure;
- records containing personal health information in its custody or control are protected against unauthorized copying or modification;
- records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.

Safeguards must be proportionate to the sensitivity of the information. This requires knowing what personal health information is in your custody or control and then determining how best to protect it, paying particular attention to personal health information that is sensitive in nature.

### **Before you go**

When you travel off-site, only take the information you need to complete your work. Whenever you take any personal health information off-site, you're exposing it to more risk than if you had left it in the office, hospital or clinic.

### **On the go**

Bags or laptops left in cars are at risk to be stolen. Consider the following questions.

- Is this personal health information something you should be leaving in your car?
- If you have to leave personal health information in your car put it out of sight.
- Personal health information might be stored on a USB flash drive. This type of device is easy to transport but is also easy to accidentally misplace. Ensure devices are password-protected and encrypted.
- To ensure information is not lost or left behind in transit, consider taking steps to remind yourself to take the information with you when you stop on your journey?

### **Once you get there**

Once you have arrived at your destination, consider how you will secure the personal health information.

### **Security for Electronic Information**

You may have a choice between taking physical documents off-site or operating off-site with an electronic device such as a laptop, smartphone, notepad, or external hard drive. If using an electronic device remember the following tips.

- Secure the device
  - Set a strong password on the device.
  - Check if the security software is up to date.
  - Check if the firewalls and current antivirus software is in place and up to date.
- Secure the personal health information on the device
  - Use password protection on documents or encrypt the information if you can.

It is the custodian's responsibility to keep personal health information secure wherever it is.

### **What if something goes wrong?**

If you find yourself dealing with a situation where personal health information has been lost or stolen, there are four key steps to take:

- containment - prevent the situation from worsening;
- evaluation - evaluate the potential harm that may be caused;

- notification - decide whether the seriousness of the situation requires you to notify people who may be affected, and
- prevention – review the incident to reduce the chances of a repeat.

### Checklist

- Do I need everything I am planning to take? If you do not need it, do not take it!
- What are my safest choices in transporting or accessing personal health information on a job?
- What can I do to make sure the personal health information I take off-site is safe and secure?
- Is there anything else I can do to make sure the personal health information remains safe while I am off-site?
- When I get to my destination, how will I store the personal health information safely?
- Do I know what to do if something goes wrong?

### *PHIA Privacy Breach Statistics November 1, 2023 – January 31, 2024*

Between November 1, 2023 and January 31, 2024, OIPC received five breach notifications from five different custodians. This is the same number of breaches reported during the previous quarter.

**We would like to remind custodians that OIPC can offer PHIA training that is customized to their needs!**

Interested custodians should email OIPC at [commissioner@oipc.nl.ca](mailto:commissioner@oipc.nl.ca).

There are also a number of PHIA resources available on OIPC's [website](#).